(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 771 875**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **97 13825**

(51) Int Cl^6 : **H 04 L 9/32**, H 04 Q 7/06

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 04.11.97.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 04.06.99 Bulletin 99/22.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *KREMER GILLES JEAN ANTOINE* — FR.

(72) **Inventeur(s) :** KREMER GILLES JEAN ANTOINE.

(73) **Titulaire(s) :**

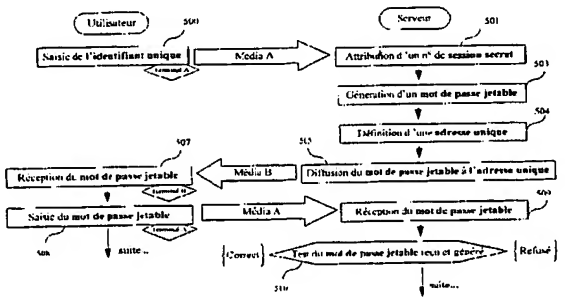
(74) **Mandataire(s) :**

(54) PROCEDE DE TRANSMISSION D'INFORMATION ET SERVEUR INFORMATIQUE LE METTANT EN OEUVRE.

(57) La présente invention propose l'utilisation combinée d'au moins deux réseaux de communication et plus précisément l'échange d'information confidentielle à un usager d'un premier support d'information à l'aide d'un deuxième support d'information via un mécanisme de synchronisation des supports d'information et de renvoi d'information d'un support à l'autre.

Le procédé de transmission d'information sur un premier support comporte ainsi:

- une opération d'ouverture d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de transmission, et, durant ladite session:
- une opération de réception d'une information confidentielle sur un terminal à adresse unique sur un deuxième support de transmission, et
- une opération de transmission, sur le premier support de transmission, d'un message confidentiel représentant l'information confidentielle.
- une opération pour vérifier si le message confidentiel correspond à l'information confidentielle.



FR 2 771 875 - A1

2771875

La présente invention concerne un procédé de transmission d'information et un serveur informatique le mettant en oeuvre. Elle s'applique, en particulier, à la vérification d'identité de la personne qui accède à un service distant, quel que soit le terminal utilisé. Elle permet d'authentifier l'identité de l'utilisateur, de délivrer un certificat de transaction, de compléter le certificat de transaction par un montant de transaction, de vérifier l'intégrité d'une transaction et d'effectuer le paiement de bien ou de service, en ligne.

Des domaines d'application de l'invention sont, par exemple, le contrôle d'accès, la remise en main propre d'information confidentielle et la certification de transactions ou de paiement de biens ou services sur un réseau.

La mise en oeuvre de la transaction à distance sur réseau pose le problème de l'authentification de la personne qui la réalise, de l'intégrité de la transaction et de sa confidentialité. Dans de nombreuses applications (commerce électronique, banque à distance, télé travail, sécurité interne des entreprises, sécurisation de bases de données payantes, par exemple) et sur tous supports (réseaux informatiques locaux ou distants (par exemple, respectivement, les réseaux communément appelés "intranet" ou "internet"), serveurs vocaux, par exemple), ce problème est crucial.

Les dispositifs et procédés de sécurisation connus dans l'art antérieur comme ceux illustrés dans le document US-A-5.442.704, qui utilisent une carte à mémoire, imposent des contraintes logicielles et matérielles importantes et coûteuses.

D'autres dispositifs utilisent un moyen d'authentification connu sous le nom "d'authentifieur" ou de "token", qui calcule à partir de données reçues au cours d'une transaction et d'une clé secrète qu'il conserve en mémoire, un mot de passe dynamique. Ces dispositifs imposent, de nouveau, des contraintes matérielles importantes et coûteuses.

La présente invention entend remédier à ces inconvénients. A cet effet, la présente invention propose l'utilisation combinée d'au moins deux réseaux de communication.

En d'autres termes, la présente invention propose l'échange d'information confidentielle à un usager d'un premier support d'information à l'aide d'un deuxième support d'information, préférentiellement sécurisé, via un mécanisme de synchronisation en temps réel des supports d'information et de renvoi d'information d'un support à l'autre.

A cet effet, la présente invention vise, selon un premier aspect, un procédé de transmission d'information sur un premier support de transmission, caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de transmission,

et, durant ladite session :

. une opération de réception d'une information confidentielle sur un terminal à adresse unique sur un deuxième support de transmission, et

. une opération de transmission, sur le premier support de transmission, d'un message confidentiel représentatif de ladite information confidentielle.

La présente invention vise, selon un deuxième aspect, un procédé de transmission d'information sur un premier support de transmission, caractérisé en ce qu'il comporte :

- une opération d'ouverture, par l'intermédiaire d'un terminal à adresse unique sur ledit premier support de transmission, d'une session de communication avec un moyen de communication situé à distance,

et, durant ladite session :

. une opération de réception d'une information confidentielle sur le premier support de transmission, et

. une opération de transmission, sur un deuxième support de transmission, d'un message confidentiel représentatif de ladite information confidentielle.

La présente invention vise, selon un troisième aspect, un procédé de transmission d'information sur un premier support de transmission, caractérisé en ce qu'il comporte :

- une opération d'ouverture, par l'intermédiaire d'un premier terminal, d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de transmission,

- une opération d'ouverture, par l'intermédiaire d'un deuxième terminal, d'une session de communication avec un moyen de communication situé à distance, sur un deuxième support de transmission,

- lorsque les deux sessions sont ouvertes, une opération de réception d'une information confidentielle sur un desdits supports de transmission sur lequel l'un des terminaux a une adresse unique, et

- une opération de transmission, sur l'autre desdits supports de transmission, d'un message confidentiel représentatif de ladite information confidentielle.

La présente invention vise, selon un quatrième aspect, un procédé de transmission d'information sur un premier support de transmission, caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de transmission,

et, durant ladite session :

. une opération de génération d'une information confidentielle et de transmission de ladite information confidentielle sur un deuxième support de transmission à un terminal possédant une adresse unique sur le deuxième support,

. une opération de réception, sur le premier support de transmission, d'un message confidentiel susceptible d'être représentatif de ladite information confidentielle, et

. une opération de vérification de correspondance entre ledit message confidentiel et ladite information confidentielle.

La présente invention vise, selon un cinquième aspect, un procédé de transmission d'information sur un support de transmission dit "deuxième", ledit

support de transmission faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un terminal dit "deuxième", d'un premier message représentatif :
  - . d'un identifiant d'un terminal dit "troisième" possédant une adresse unique sur ledit réseau,
  - . d'une information confidentielle,
  - . d'une information représentative d'un montant de transaction,
- une opération de transmission, au troisième terminal, d'un deuxième message représentatif :
  - . de ladite information confidentielle et
  - . dudit montant,
- une opération de réception d'un troisième message, de la part dudit deuxième terminal, représentatif d'une validation de transaction, et
- une opération d'incrémentation d'un registre correspondant audit troisième terminal, d'une valeur représentative dudit montant de transaction.

La présente invention vise, selon un sixième aspect, un procédé de transmission d'information sur un support de transmission dit "deuxième", ledit support de transmission faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un terminal dit "deuxième", d'un premier message représentatif :
  - . d'un identifiant d'un terminal dit "troisième" possédant une adresse unique sur ledit réseau,
  - . d'une information confidentielle,
  - . d'une information représentative d'un montant de transaction,
- une opération de transmission, au troisième terminal, d'un deuxième message représentatif :
  - . de ladite information confidentielle et
  - . dudit montant,
- une opération de réception d'un troisième message, de la part dudit deuxième terminal, représentatif d'une validation de transaction, et

- une opération d'incrémentation d'un registre correspondant audit troisième terminal, d'une valeur représentative d'une durée de la première session.

On observe que, selon les cinquième et sixième aspects, de l'invention, l'opération d'incrémentation peut avoir lieu avant ou après l'opération de réception d'un troisième message.

La présente invention vise, selon un septième aspect, un procédé de transmission d'information sur un support de transmission dit "deuxième", ledit support de transmission faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un terminal dit "deuxième", d'un premier message représentatif :

. d'un identifiant d'un terminal dit "troisième" possédant une adresse unique sur ledit réseau,

. d'une information confidentielle,

. d'une information représentative d'un montant de transaction,

- une opération de transmission, au troisième terminal, d'un deuxième message représentatif :

. de ladite information confidentielle et

. dudit montant,

- une opération d'incrémentation d'un registre correspondant audit troisième terminal, d'une valeur prédéterminée.

La présente invention vise, selon un huitième aspect, un procédé de transmission d'information, entre un premier terminal et un deuxième terminal, sur un premier support de transmission appartenant à un réseau de communication, caractérisé en ce qu'il comporte :

- une opération d'ouverture de session de communication, sur le premier support de transmission entre le premier terminal et le deuxième terminal, et

- une opération de transmission, de la part du deuxième terminal à un troisième terminal raccordé à un deuxième réseau et possédant une adresse unique sur ledit deuxième réseau, d'un premier message représentatif d'une information confidentielle,

- une opération de transmission, au troisième terminal, d'un deuxième message représentatif de ladite information confidentielle, et

- une opération de transmission, sur le premier support de transmission, en provenance du premier terminal et à destination du deuxième terminal, d'un message représentatif de l'information confidentielle.

Selon des caractéristiques particulières de chacun des aspects de la présente invention exposés ci-dessus :

- l'information confidentielle est représentative d'un montant de transaction,

- l'information confidentielle est représentative d'un nombre pseudo-aléatoire,

- l'information confidentielle est représentative d'un numéro de session attribué à une session,

- l'information confidentielle est représentative de l'identifiant de l'utilisateur,

- l'information confidentielle est représentative d'un ou plusieurs numéros de compte bancaire et/ou de carte,

- l'information confidentielle est représentative de l'heure et la date de ladite opération d'ouverture de session, et/ou

- l'information confidentielle est modifiée à chacune des sessions.

Grâce à chacune de ces dispositions, l'information confidentielle est renouvelée à chaque session et son usage est limité à une seule session de communication.

La présente invention vise, en outre, un serveur informatique, caractérisé en ce qu'il est adapté à mettre en oeuvre le procédé de transmission tel que succinctement exposé ci-dessus.

Ce serveur présentant les mêmes avantages que les procédés succinctement exposés ci-dessus, ces avantages ne sont pas rappelés ici.

D'autres avantages, buts et caractéristiques de l'invention ressortiront de la description qui va suivre, faite en regard des dessins annexés dans lesquels :

- la figure 1 est un schéma de principe du procédé de la présente invention ;

- la figure 2 représente un schéma général de mise en oeuvre de la présente invention ;

- la figure 3 représente une architecture matérielle et logicielle capable de supporter la mise en oeuvre de la présente invention ;

- la figure 4 représente une succession d'opérations génériques mises en oeuvre par les éléments illustrés en figures 2 et 3 ;

- la figure 5 représente une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans le cadre d'une application de la présente invention à l'authentification; et

- la figure 6 représente une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans le cadre d'une application de la présente invention à la certification de messages ;

- la figure 7 représente une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans le cadre d'une application de la présente invention au paiement électronique en ligne, dans le cas d'un service sans abonnement ;

- la figure 8 représente une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans le cadre d'une application de la présente invention au paiement électronique en ligne, dans le cas d'un service avec abonnement ; et

- la figure 9 représente une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans le cadre d'une application de la présente invention au paiement avec un terminal de paiement électronique connu.

En figure 1 sont représentés :

- un premier réseau 10,
- un premier terminal de premier réseau 11,
- un deuxième terminal de réseaux serveur de données et de messages 40,
- un deuxième réseau 20,
- un troisième terminal de deuxième réseau 21, et

- un serveur d'information 30.

Selon l'invention, l'utilisateur du premier terminal 11 est identifié par son adresse unique sur le deuxième réseau 20. Celui-ci est donc préférentiellement sécurisé, c'est-à-dire que chaque adresse y est certifiée par un tiers de confiance, et, en outre, l'information transmise est cryptée. Le tiers considéré est préférentiellement un opérateur de téléphonie.

Le terminal de premier réseau 11 peut être, par exemple, un téléphone, un terminal informatique, un télécopieur, un terminal télématique, un téléviseur équipé d'un boîtier adapté à recevoir et à émettre des données informatiques (boîtier communément appelé un décodeur TV), un terminal de paiement électronique (figure 2).

Le terminal de deuxième réseau 21 peut être, par exemple, un téléphone, un télécopieur, un terminal télématique, un décodeur TV, un téléphone mobile ou un récepteur de messages ("pageur") ou un assistant personnel numérique (communément appelé "PDA").

Dans un premier temps, l'utilisateur utilise le terminal 11 de premier réseau 10 pour entrer en communication avec le serveur d'information 30. Il ouvre ainsi une session de communication. Ensuite, le serveur d'information 30 fournit une information confidentielle à l'utilisateur, par l'intermédiaire :

- du serveur de données et de messages 40,
- du deuxième réseau 20 et
- du terminal de deuxième réseau 21,

Enfin, l'utilisateur transmet au serveur d'information 30, un message confidentiel représentatif de l'information confidentielle, au cours de la même session, par l'intermédiaire :

- du terminal de premier réseau 11 et
- du premier réseau 10.

Le serveur de données et de messages 40 vérifie la correspondance du message confidentiel et de l'information confidentielle, c'est-à-dire si le message confidentiel est représentatif de l'information confidentielle, et, en cas de correspondance, il donne l'accès à des services particuliers, payants ou confidentiels.

En figure 2 sont représentés :

- un premier terminal, dit "utilisateur" 100 relié à un premier support de communication 101 faisant partie d'un réseau de communication ;

- un serveur d'information 103, relié au premier support d'information 101 ;

- un serveur de données 105, relié par une ligne informatique 106 au serveur d'information 103 ;

- un serveur de messages 109, reliée par un deuxième support de communication 110 à un récepteur 111 et par un troisième support de communication 113, au serveur de données 105 ; et

- une base de données d'abonnés 107 reliée au serveur de message 109 et au serveur de données 105.

Dans le mode de réalisation décrit et représenté, le terminal utilisateur 100 est un ordinateur personnel (communément appelé « PC ») ou un ordinateur de réseau (communément appelé « NC »), ou encore un Minitel (marque déposée) qui comporte un modem relié à un réseau de téléphone filaire, comme par exemple le réseau téléphonique commuté. Le premier support de communication 101 est donc un canal de ce réseau téléphonique. Le terminal utilisateur met en oeuvre un logiciel de communication de type connu, qui lui permet de communiquer à distance avec le serveur d'information 103, par l'intermédiaire du support de communication 101.

Le serveur d'information 103, relié au premier support d'information 101 est un serveur informatique de type connu, qui est ici adapté à mettre en oeuvre un logiciel spécifique, conforme à l'invention (illustré en l'une des figures 4 à 9).

Le serveur de données 105 est un serveur informatique de type connu qui fonctionne comme il est indiqué ci-dessous, en relation avec le serveur d'information 103, par l'intermédiaire de la ligne informatique 106, elle aussi de type connu.

Le serveur de messages 109 est un système informatique de type connu qui gère un ou des réseaux de communication de types connus, un canal de l'un de ces réseaux constituant un deuxième support de communication. Un canal spécialisé fournit le troisième support 113 pour la communication entre le serveur d'information 103 et le serveur de messages 109.

La base de données d'abonnés 107 est un registre de mémoire de type connu.

Le réseau 110 est un réseau de communication de type connu. Dans ce deuxième réseau, chaque récepteur possède une adresse unique qui est certifiée au moment de l'attribution de l'adresse du récepteur 111.

Le récepteur 111 est, dans le mode de réalisation décrit et représenté ici, un téléphone portable (communément appelé "mobile") ou un récepteur de message (communément appelé « pageur »), un télécopieur ou un téléphone fixe ou un terminal équipé d'un modem. Il est adapté à recevoir un message confidentiel et à le mettre à disposition de l'utilisateur, par exemple par affichage, émission vocale ou impression sur papier. En variante, les serveurs d'information 103 et le serveur de messages 109 sont confondus.

En figure 3, on observe, dans une architecture matérielle et logicielle permettant la mise en oeuvre de la présente invention, un terminal informatique 301, un réseau informatique 302, un serveur d'information 303, un réseau local 304, un serveur d'authentification 305, une base de données 306, un serveur de messages 307, un réseau 308, un moyen de diffusion 309, un réseau de radiotéléphonie 310, un réseau de téléphonie cellulaire 311, un récepteur de messages alphanumériques 312 et un téléphone mobile 313, un réseau commuté 314 et un téléphone ou télécopieur 315.

Le terminal informatique 301 est, par exemple un micro-ordinateur connu sous le nom de "PC". Il comporte un modem permettant la communication en émission et en réception, avec le réseau informatique 302. Le réseau informatique 302 est le réseau informatique mondial connu sous le nom d'"internet". Le serveur d'information 303 est de type connu pour la mise en oeuvre de sites de fournisseurs de services sur le réseau 302.

Le réseau local 304 est de type connu. C'est un réseau d'entreprise.

Le serveur d'authentification 305 et le serveur de message 307 sont de types connus. La base de données 306 est de type connu.

Le réseau 308 est de type connu.

Le moyen de diffusion 309 est un émetteur hertzien, de type connu pour la mise en oeuvre de réseau de communication mobile. Il est, par exemple cellulaire ou par satellite.

Dans le mode de réalisation décrit et représenté en figure 3, l'un des trois réseaux de communication suivants est utilisé :

- le réseau de radiotéléphonie 310 qui ne permet que la communication dans le sens de la diffusion depuis un émetteur vers des récepteurs de messages alphanumériques comme le récepteur 312, sans que ceux-ci ne puissent émettre de signaux à distance,

- un réseau de téléphonie mobile 311, permettant la communication en particulier avec des téléphones mobiles, comme le téléphone 313, et

- un réseau commuté 314 permettant ici la communication avec un téléphone fixe ou un télécopieur fixe 315.

Ces trois réseaux fonctionnent par abonnement, avec certification de l'identité de l'abonné. Ce récepteur possède une adresse unique sur le réseau considéré, c'est-à-dire que l'adresse qui lui est attribuée n'est pas attribuée à un récepteur (sauf dans certains cas d'abonnements groupés demandés par l'utilisateur). Cette adresse unique s'apparente à un numéro de téléphone.

Dans le cas illustré en figure 3, c'est préférentiellement le même utilisateur qui met en oeuvre le terminal informatique 301, le récepteur alphanumérique 312, le téléphone mobile 313, le télécopieur fixe ou le téléphone fixes.

Les figures 4 à 9 qui illustrent différentes applications de la présente invention, utilisent le même formalisme : sur chacune de ces figures, les opérations sont représentées de haut en bas, dans l'ordre de leur succession chronologique. Sur ces figures, sont représentées :

- sur la colonne verticale la plus à gauche et sous forme de rectangles, les opérations effectuées par l'utilisateur, en mettant en oeuvre soit le terminal relié au premier réseau ("terminal A") soit le terminal relié au deuxième réseau ("terminal B"), le terminal est inscrit dans un losange auquel le rectangle représentant l'opération considérée se superpose ;

- sur une colonne centrale, des transmissions d'information successives sur réseau (A ou B), sous forme de flèches dont le sens correspond au sens de communication, c'est-à-dire que le sens de gauche à droite, correspond au sens utilisateur vers serveur et que le sens de droite à gauche correspond au sens serveur vers utilisateur. On observe ici que pour chaque transmission d'information, plusieurs signaux peuvent être échangés entre les systèmes électroniques mis en oeuvre (synchronisation, sélection de protocole de communication, information, redondances, acquittement de transmission, retransmission en cas d'erreur de transmission, ...). Dans ces flèches, le serveur "A" correspond au premier réseau et le serveur "B" au deuxième réseau ;

- sur une colonne verticale plus à droite que les deux précédentes (la plus à droite en figures 4 à 6 et 9), sous forme de rectangles, les opérations effectuées par le serveur de données 105 ; et

- en figures 7 et 8, sur une colonne verticale située la plus à droite, un serveur mis en communication avec le serveur de données 105.

En figure 4, on observe une succession d'opérations génériques mises en oeuvre par les éléments illustrés en figures 2 et 3 :

- au cours d'une opération 200, l'utilisateur du terminal utilisateur 101 entre en communication avec le serveur d'information 103, par l'intermédiaire du premier support de communication. Au cours de cette opération 200, il fournit un identifiant unique (par exemple un numéro d'abonné, un nom ou une adresse physique) ;

- au cours de l'opération 201, le serveur d'information 103 attribue un numéro de session unique dès la connexion du terminal "utilisateur" 100 au serveur d'information 103. Au cours de cette opération 201, le serveur d'information 103 transmet l'identifiant au serveur de données 105 ;

- au cours de l'opération 202, le serveur de données 105 calcule une information confidentielle aussi appelée par la suite "secret", au serveur de messages 109. A cet effet, le serveur de données 105 calcule le secret à partir d'un invariant (l'identifiant, par exemple), d'un variant pour éviter les répétitions (numéro de session, par exemple) et d'un marqueur temporel (l'horloge) afin de borner l'utilisation d'un secret dans le temps. Préférentiellement, il met en oeuvre une

fonction de calcul d'information confidentielle (ou "secret") irréversible, c'est-à-dire dont on ne peut retrouver l'information d'entrée lorsque l'on connaît celle de sortie. Pour la mise en oeuvre de l'opération 202, le lecteur pourra se référer à des livres d'algorithmes de sécurité bien connus, et en particulier aux descriptions des fonctions connues sous les noms de "hashing", "Message Digest", et "SHA";

- l'opération 203 prend plusieurs formes différentes selon que l'identifiant est déjà dans la base de données ou non : dans l'affirmative, l'adresse unique y est lue, dans la négative, il est fait appel au tiers certificateur qui est, ici, l'opérateur du deuxième réseau ;

- au cours de l'opération 204, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant transmis par le serveur d'information 103 au serveur de message 109, au cours de l'opération 203 ;

- au cours de l'opération 205, le serveur de messages 109 transmet, par l'intermédiaire du réseau 110, l'information confidentielle transmise au cours de l'opération 203 au récepteur 111 qui possède ladite adresse unique ;

- au cours de l'opération 207, l'information confidentielle, aussi appelée ici "secret" est fournie à l'utilisateur, soit en étant affichée sur l'afficheur du récepteur 111, soit en étant donnée de manière vocale ou télécopiée ;

- au cours de l'opération 208, l'utilisateur fournit au serveur d'information 103, qui, lui-même, le retransmet au serveur de données 105, un message confidentiel représentatif de l'information confidentielle (par exemple identique à cette information confidentielle ou "secret"), par l'intermédiaire du clavier du terminal utilisateur 100 ;

- au cours de l'opération 209, le serveur d'information 103 reçoit ce message confidentiel ;

- au cours du test 210, le serveur de données 105 détermine si ce message confidentiel est représentatif de l'information confidentielle générée par le serveur de données 105, au cours de l'opération 202, ou non ;

- lorsque le résultat du test 210 est positif, le serveur de données 105 donne à l'utilisateur l'accès aux ressources protégées ;

- lorsque le résultat du test 210 est négatif, le serveur de données 105 transmet, à l'utilisateur, un message d'erreur, en précisant éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et l'accès aux ressources protégées est refusé à l'utilisateur.

Enfin, la fin de la session est de type connu.

On observe ici que même si le secret était divulgué à un tiers, du fait que ce secret correspond au numéro de session unique attribué dynamiquement par le serveur d'information 103 et du fait que la session reste ouverte (mode connecté) jusqu'à l'envoi du secret, ce tiers ne pourrait pas abuser du secret pour réaliser des opérations frauduleuses.

En figure 5, on observe une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans une application de l'invention à l'authentification, pour accès à des données protégées :

- au cours d'une opération 500, l'utilisateur du terminal utilisateur 101 entre en communication avec le serveur d'information 103, par l'intermédiaire du premier support de communication. Au cours de cette opération 500, il fournit un identifiant unique (par exemple un numéro d'abonné, un nom, ou une adresse physique) ;

- au cours de l'opération 501, le serveur d'information 103 attribue un numéro de session unique dès la connexion du terminal utilisateur au serveur d'information 103. Au cours de cette opération 501, le serveur d'information 103 transmet l'identifiant au serveur de données 105 ;

- au cours de l'opération 502, le serveur de données 105 calcule une information confidentielle aussi appelée par la suite "mot de passe jetable", au serveur de messages 109. A cet effet, le serveur de données 105 calcule l'information confidentielle à partir d'un invariant (l'identifiant, par exemple), d'un variant pour éviter les répétitions (numéro de session, par exemple) et d'un marqueur temporel (l'horloge) afin de borner l'utilisation d'un secret dans le temps. Préférentiellement, il met en oeuvre une fonction de calcul d'information confidentielle irréversible, c'est-à-dire dont on ne peut retrouver l'information d'entrée lorsque l'on connaît celle de sortie. Pour la mise en oeuvre de l'opération 502, le lecteur pourra se référer aux livres mentionnés plus haut ;

- au cours de l'opération 504, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant transmis par le serveur d'information 103 au serveur de message 109, au cours de l'opération 503 ;

- au cours de l'opération 505, le serveur de messages 109 transmet, par l'intermédiaire du réseau 110, l'information confidentielle aussi appelée ici "mot de passe jetable", au cours de l'opération 503 au récepteur 111 qui possède ladite adresse unique ;

- au cours de l'opération 507, l'information confidentielle, aussi appelée ici "mot de passe jetable" est fournie à l'utilisateur, soit en étant affichée sur l'afficheur du récepteur 111, soit en étant donnée de manière vocale ou télécopiée ;

- au cours de l'opération 508, l'utilisateur fournit au serveur d'information 103, qui, lui-même, le retransmet au serveur de données 105, un message confidentiel représentatif de l'information confidentielle (par exemple identique à cette information confidentielle, ou "mot de passe jetable"), par l'intermédiaire du clavier du terminal utilisateur 100 ;

- au cours de l'opération 509, le serveur d'information 103 reçoit ce message confidentiel ;

- au cours du test 510, le serveur de données 105 détermine si ce message confidentiel est représentatif de l'information confidentielle générée par le serveur de données 105, au cours de l'opération 503, ou non ;

- lorsque le résultat du test 510 est positif, le serveur de données 105 valide l'accès à l'information protégée ;

- lorsque le résultat du test 510 est négatif, le serveur de données 105 transmet un message d'erreur et d'invalidation d'accès, en précisant éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et l'accès à l'information protégée est refusé.

Enfin, la fin de la session est de type connu.

En figure 6, on observe une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans une application de l'invention à la certification de message :

- au cours d'une opération 600, l'utilisateur du terminal "utilisateur" 100 entre en communication avec le serveur d'information 103, par l'intermédiaire du premier support de communication. Au cours de cette opération 200, il initie une procédure de transaction (par exemple virement de compte à compte, commande ou ordre boursier) (voir ci-dessus en regard de la figure 4) ;

- au cours de l'opération 601, le serveur d'information 103 attribue un numéro de session unique secret ;

- au cours de l'opération 603, le serveur de données 105 calcule une information confidentielle aussi appelée, par la suite, "certificat de message" à partir d'un invariant (l'identifiant, par exemple), d'un variant pour éviter les répétitions (numéro de session, par exemple) et d'un marqueur temporel (l'horloge) afin de borner l'utilisation d'un secret dans le temps. Préférentiellement, il met en oeuvre une fonction de calcul d'information confidentielle irréversible, c'est-à-dire dont on ne peut retrouver l'information d'entrée lorsque l'on connaît celle de sortie. Pour la mise en oeuvre de l'opération 603, le lecteur pourra se référer aux livres mentionnés plus haut ;

- au cours de l'opération 604, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant transmis, par le serveur d'information 103, au serveur de message 109, au cours de l'opération 603 ;

- au cours de l'opération 605, le serveur de messages 109 transmet, par l'intermédiaire du réseau 110, l'information confidentielle aussi appelée ici "certificat de message", transmis au cours de l'opération 603 au récepteur 111 qui possède ladite adresse unique ;

- au cours de l'opération 607, l'information confidentielle, aussi appelée ici "certificat de message" est fournie à l'utilisateur, soit en étant affichée sur l'afficheur du récepteur 111, soit en étant donnée de manière vocale ou télécopiée ;

- au cours de l'opération 608, l'utilisateur fournit au serveur d'information 103, qui, lui-même, le retransmet au serveur de données 105, un message confidentiel représentatif de l'information confidentielle (par exemple identique à cette information confidentielle, ou "certificat de message"), par l'intermédiaire du clavier du terminal utilisateur 100 ;

- au cours de l'opération 609, le serveur d'information 103 reçoit ce message confidentiel ;

- au cours du test 610, le serveur de données 105 détermine si ce message confidentiel est représentatif de l'information confidentielle générée par le serveur de données 105, au cours de l'opération 603, ou non ;

- lorsque le résultat du test 610 est positif, le serveur de données 105 valide la transaction effectuée, puis reprend ;

- lorsque le résultat du test 610 est négatif, le serveur de données 105 transmet un message d'erreur et d'invalidation de transaction, en précisant éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et ne réalise pas la transaction.

Enfin, la fin de la session est de type connu.

Selon une variante :

- au cours de l'opération 603, le "certificat de message" est aussi déterminé, par le serveur de données 105, à partir d'un montant d'un virement et/ou d'un numéro de compte bancaire émetteur et/ou d'un numéro de compte bancaire récepteur,

- au cours de l'opération 605, le serveur de messages 109 transmet, par l'intermédiaire du réseau 110, l'information confidentielle et le montant du virement, en clair ; et

- au cours de l'opération 607, l'information confidentielle ainsi que le montant sont fournis à l'utilisateur qui vérifie l'intégrité du montant du virement en cours.

En figure 7, on observe une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans une application de l'invention au paiement électronique en ligne, dans le cas d'un service sans abonnement :

- à la suite d'une opération d'ouverture de session, non représentée, entre le terminal utilisateur 100 et le serveur d'information 103,

- au cours de l'opération 700, le serveur d'information 103 attribue un numéro de session unique secret ;

- au cours d'une opération 701, le serveur d'information 103 reçoit de la part du terminal utilisateur 100, un identifiant ;

- au cours d'une opération 702, l'utilisateur du terminal utilisateur 101 choisit un bien ou un service dont il souhaite avoir le bénéfice, puis initie une procédure de paiement (voir ci-dessus en regard de la figure 4) ;

- au cours de l'opération 703, le serveur de données 105 reçoit la demande de paiement de la part du terminal utilisateur 100 ;

- au cours de l'opération 704, l'utilisateur fournit au serveur d'information 103 de l'information confidentielle concernant sa carte de paiement ;

- au cours de l'opération 705, le serveur de données 105 effectue une demande d'autorisation bancaire au serveur 706 d'une banque où l'utilisateur dispose du compte auquel est rattaché la carte de paiement concernée par l'opération 704. Il fournit le montant de la transaction envisagée au serveur bancaire 706. Le serveur d'information 103 reçoit, en retour, de la part du serveur de banque 706, une autorisation de paiement, selon des modalités bancaires qui dépendent du montant disponible sur le compte bancaire considéré et de l'éventuelle autorisation de découvert sur ledit compte ;

- au cours d'une opération 707, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant transmis par le serveur d'information 103 au serveur de message 109, au cours de l'opération 701 ;

- au cours d'une opération 708, le serveur d'information 103 calcule une information confidentielle aussi appelée, par la suite "certificat de transaction" à partir :

. d'un invariant (l'identifiant, par exemple),

. d'un variant pour éviter les répétitions (numéro de session, par exemple),

. du montant de la transaction et

. d'un marqueur temporel (l'horloge) afin de borner l'utilisation d'un secret dans le temps.

Préférentiellement, il met en oeuvre une fonction de calcul d'information confidentielle irréversible, c'est-à-dire dont on ne peut retrouver l'information d'entrée lorsque l'on connaît celle de sortie. Pour la mise en oeuvre de l'opération 708, le lecteur pourra se référer aux livres mentionnés plus haut. Au cours

de cette opération 708, le certificat de transaction et le montant de la transaction envisagée sont diffusés, par l'intermédiaire du réseau 110, au récepteur 111 qui possède ladite adresse unique ;

- au cours de l'opération 709, l'information confidentielle, aussi appelée ici "certificat de transaction" est fournie à l'utilisateur, conjointement au montant de la transaction, en clair, soit en étant affichée sur l'afficheur du récepteur 111, soit en étant donnée de manière vocale ou télécopiée, ce qui permet le contrôle par l'utilisateur de l'intégrité de la transaction qu'il réalise ;

- au cours de l'opération 710, l'utilisateur fournit au serveur d'information 103, qui, lui-même, le retransmet au serveur de données 105, un message confidentiel identique à, ou, en variante, représentatif de, l'information confidentielle constituée par le certificat de transaction, par l'intermédiaire du clavier du terminal utilisateur 100 ;

- au cours de l'opération 711, le serveur d'information 103 reçoit ce message confidentiel ;

- au cours du test 712, le serveur de données 105 détermine si ce message confidentiel est représentatif de l'information confidentielle générée par le serveur de données 105, au cours de l'opération 708, ou non ;

- lorsque le résultat du test 712 est positif, le serveur de données 105 valide le paiement effectué, ce paiement étant effectivement réalisé entre les organismes bancaires selon des techniques connues, puis reprend le fonctionnement de présentation d'offres commerciales ;

- lorsque le résultat du test 712 est négatif, le serveur de données 105 transmet à l'utilisateur un message d'erreur et d'invalidation du paiement, en précisant éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et le paiement n'est pas effectué.

Enfin, la fin de la session est de type connu.

En variante du mode de réalisation illustré en figure 7, l'opération 705 est effectuée après toutes les autres opérations, mais avant la fin de session.

En figure 8, on observe une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans une application de l'invention au paiement électronique en ligne, dans le cas d'un service avec abonnement :

- à la suite d'une opération d'ouverture de session, non représentée, entre le terminal utilisateur 100 et le serveur d'information 103,

- au cours de l'opération 800, le serveur d'information 103 attribue un numéro de session unique secret ;

- au cours d'une opération 801, le serveur d'information 103 reçoit de la part du terminal utilisateur 100, un identifiant ;

- au cours d'une opération 802, l'utilisateur du terminal utilisateur 101 choisit un bien ou un service dont il souhaite avoir le bénéfice, puis initie une procédure de paiement (voir ci-dessus en regard de la figure 4) ;

- au cours de l'opération 803, le serveur de données 105 reçoit la demande de paiement de la part du terminal utilisateur 100 ;

- au cours de l'opération 805, le serveur de données 105 effectue, préférentiellement de manière sécurisée, une demande d'autorisation bancaire au serveur 706 d'une banque où l'utilisateur dispose du compte auquel est rattaché la carte de paiement concernée par l'opération 804. Il fournit le montant de la transaction envisagée au serveur bancaire 806 ainsi que des données concernant la carte de paiement, ces données étant conservées par le serveur d'information 103 à compter de l'abonnement de l'utilisateur au service considéré. Le serveur d'information 103 reçoit, en retour, de la part du serveur de banque 806, une autorisation de paiement, selon des modalités bancaires qui dépendent du montant disponible sur le compte bancaire considéré et de l'éventuelle autorisation de découvert sur ledit compte ;

- au cours d'une opération 807, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant transmis par le serveur d'information 103 au serveur de message 109, au cours de l'opération 801 ;

- au cours d'une opération 808, le serveur d'information 103 calcule une information confidentielle aussi appelée, par la suite, "certificat de transaction" (voir figure 7) ;

- au cours de l'opération 809, l'information confidentielle, aussi appelée ici "certificat de transaction" est fournie à l'utilisateur, conjointement au montant de la transaction, en clair, soit en étant affichée sur l'afficheur du récepteur 111, soit en étant donnée de manière vocale ou télécopiée, ce qui permet le contrôle de l'intégrité de la transaction par l'utilisateur ;

- au cours de l'opération 810, l'utilisateur fournit au serveur d'information 103, qui, lui-même, le retransmet au serveur de données 105, un message confidentiel identique à, ou, en variante, représentatif de, l'information confidentielle constituée par le certificat de transaction, par l'intermédiaire du clavier du terminal utilisateur 100 ;

- au cours de l'opération 811, le serveur d'information 103 reçoit ce message confidentiel ;

- au cours du test 812, le serveur de données 105 détermine si ce message confidentiel est représentatif de l'information confidentielle générée par le serveur de données 105, au cours de l'opération 808, ou non ;

- lorsque le résultat du test 812 est positif, le serveur de données 105 valide le paiement effectué, ce paiement étant ensuite effectivement réalisé entre les organismes bancaires selon des techniques connues, puis reprend le fonctionnement de présentation d'offres commerciales ;

- lorsque le résultat du test 812 est négatif, le serveur de données 105 transmet à l'utilisateur un message d'erreur et d'invalidation du paiement, en précisant éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et le paiement n'est pas effectué.

Enfin, la fin de la session est de type connu.

En variante du mode de réalisation illustré en figure 8, l'opération 805 est effectuée après toutes les autres opérations, mais avant la fin de session.

En figure 9, on observe une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans une application de l'invention au paiement avec un terminal de paiement électronique :

- au cours d'une opération 915, l'utilisateur introduit sa carte de paiement dans un terminal électronique de paiement ("TPE") qui constitue le terminal dit "utilisateur" ;

- au cours d'une opération 916, le commerçant saisit le montant de la transaction sur ledit TPE ;

- au cours d'une opération 900, une ouverture de session est effectuée entre le TPE 100, et le serveur d'information 103 et un numéro de session unique et secret est attribué par le serveur de communication 103 ;

- au cours d'une opération 901, le serveur d'information 103 reçoit de la part du TPE 100, des informations portées par la carte de paiement ainsi que le montant de la transaction en cours, et le serveur d'information transmet une demande de l'identifiant du consommateur auprès de l'organisme bancaire 906 et reçoit cet identifiant en retour ;

- au cours d'une opération 907, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant transmis au cours de l'opération 901 ;

- au cours d'une opération 908, le serveur d'information 103 calcule une information confidentielle aussi appelée, par la suite, "certificat de transaction" (voir figure 7) ;

- au cours de l'opération 909, l'information confidentielle, aussi appelée ici "certificat de transaction" est fournie à l'utilisateur, conjointement au montant de la transaction, en clair, soit en étant affichée sur l'afficheur du récepteur 111, soit en étant donnée de manière vocale, ce qui permet le contrôle de l'intégrité de la transaction par l'utilisateur ;

- au cours de l'opération 910, l'utilisateur fournit au serveur d'information 103, qui, lui-même, le retransmet au serveur de données 105, un message confidentiel identique à, ou, en variante, représentatif de, l'information confidentielle constituée par le certificat de transaction, par l'intermédiaire du clavier du TPE 100 ;

- au cours de l'opération 911, le serveur d'information 103 reçoit ce message confidentiel ;

- au cours du test 912, le serveur de données 105 détermine si ce message confidentiel est représentatif de l'information confidentielle générée par le serveur de données 105, au cours de l'opération 908, ou non ;

- lorsque le résultat du test 912 est positif, le serveur de données 105 valide le paiement effectué, ce paiement étant ensuite effectivement réalisé entre les organismes bancaires selon des techniques connues ;

- lorsque le résultat du test 912 est négatif, le serveur de données 105 transmet à l'utilisateur un message d'erreur et d'invalidation du paiement, en précisant éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et le paiement n'est pas effectué.

Une variante de l'opération 916 est la saisie par l'utilisateur de son code personnel aussi appelé "PIN", avant le lancement de l'opération 900.

Enfin, la fin de la session est de type connu et le client récupère sa carte de paiement ainsi qu'un ticket imprimé portant le montant du paiement effectué.

Les différents modes de réalisation de la présente invention (authentification, certification de message et paiement électronique en ligne) peuvent être combinés afin de réaliser des applications spécifiques correspondant aux exigences de l'opérateur du service.

L'invention s'applique notamment :

- au contrôle d'accès sur site informatique (pour la sécurité interne à une entreprise, pour le télétravail dans une entreprise, ...),

- à la remise d'information confidentielle en main propre (pour le courrier électronique, la télécopie sécurisée et/ou recommandée, pour la certification de devis ou de bon de commande ...),

- au paiement en ligne (pour le commerce électronique, pour la distribution d'information et ou de logiciels, ...),

- à la certification de message (pour la déclaration à distance, pour la banque à domicile, ...),

- à la remise de propositions commerciales personnalisées (pour les boîtes aux lettres sécurisées, ...),

- à la prise de pari, en ligne (pour les loteries ou les mises pour jeu de casinos, courses, ...),

- à la commande et à la réservation d'un programme de télévision (pour la télévision à facturation des seules émissions vues),

Quelques unes de ces applications sont détaillées ci-dessous, à titre d'exemple.

Pour le contrôle d'accès, le réseau utilisé peut être un réseau connu sous le nom d'"intranet" ou un réseau mondial connu sous le nom d'"internet". L'objectif de cette application de l'invention est de s'assurer que l'utilisateur est une personne habilitée.

Dans cette application :

- l'utilisateur se met en relation avec le service,

- il s'identifie en fournissant un identifiant,

- il reçoit, par l'intermédiaire d'un deuxième support de transmission (par exemple téléphone portable ou pageur), un mot de passe jetable,

- il tape ce mot de passe jetable sur le clavier de son terminal, puis

- si l'authentification est réalisée, il accède à la ressource considérée (pour la sécurité interne dans une entreprise, pour le télétravail ...).

Pour le courrier électronique ou la télécopie recommandée, le réseau utilisé peut être un réseau commuté. Les objectifs de cette application de l'invention sont :

- de s'assurer que la personne à qui est adressé le message sécurisé (le "destinataire"), le reçoit en main propre et

- de délivrer un certificat de message à l'émetteur et au destinataire du message sécurisé.

Dans cette application :

- l'utilisateur émetteur du message sécurisé compose le numéro d'un service spécialisé pour la mise en oeuvre de cette application,

- il s'identifie en fournissant un identifiant,

- il tape les coordonnées de l'utilisateur destinataire (numéro de téléphone, préférentiellement portable, adresse, télécopie, ...), puis

- il délivre son message sécurisé (oral, écrit et/ou par l'intermédiaire d'un télécopieur).

- il reçoit, par l'intermédiaire d'un deuxième support de transmission (par exemple téléphone portable ou pageur), un certificat de message,

- il tape ce certificat de message sur le clavier de son terminal, sur le premier réseau,

- ce certificat de message est vérifié,

Ensuite, l'utilisateur destinataire :

- est informé qu'un message sécurisé l'attend (cette opération est réalisée par tout moyen connu (téléphonie, télécopie, courrier, pageur, courrier électronique ...),

- il compose le numéro du service spécialisé pour la mise en oeuvre de cette application,

- il s'identifie en fournissant un identifiant,

- il reçoit, par l'intermédiaire d'un deuxième support de transmission (par exemple téléphone portable ou pageur), un certificat de message, et

- il tape ce certificat de message sur le clavier de son terminal, sur le premier réseau,

- ce certificat de message est vérifié,

- l'utilisateur destinataire du message sécurisé reçoit ce dernier,

- l'utilisateur émetteur est informé que le message sécurisé a été retiré par le destinataire.

Le service spécialisé conserve une trace de chacun des certificats ainsi délivrés.

Pour l'application de l'invention à la télédéclaration, le premier réseau utilisé peut être un réseau mondial connu sous le nom d'"internet". L'objectif de cette application de l'invention est de permettre une déclaration administrative officielle immédiate, de délivrer un récépissé à l'utilisateur et de s'assurer de l'identité du déposant.

Dans cette application :

- l'utilisateur émetteur de la déclaration se connecte à un service administratif adapté à cette application (voir ci-dessus),

- il s'identifie en fournissant un identifiant,

- il effectue ladite déclaration ou rempli un formulaire administratif,

- il reçoit, par l'intermédiaire d'un deuxième support de transmission (par exemple téléphone portable ou pageur), un certificat de message, et

- il tape ce certificat de message sur le clavier de son terminal.

Pour l'application de l'invention à l'achat et/ou le paiement en ligne, le réseau utilisé est le réseau mondial connu sous le nom d'"internet" et un logiciel mis en oeuvre par l'ordinateur de l'utilisateur permet de crypter un numéro de compte ou de carte bancaire (par exemple avec un cryptage de type connu sous le nom de "Secure Socket Level" ou "SSL"). L'objectif de cette application de l'invention est de pouvoir payer en ligne en authentifiant la personne qui réalise la transaction.

Dans cette application :

- l'utilisateur se met en relation avec une "galerie marchande", c'est-à-dire un site rassemblant des commerçants fournissant des biens, des services ou de l'information,

- il s'identifie en fournissant un identifiant,

- il choisit une transaction qu'il souhaite effectuer,

- il indique un mode de paiement (carte bancaire, par exemple),

- il envoi au serveur de la galerie marchande son numéro de carte et la date de péremption de cette carte, sous protocole de cryptage SSL,

- le serveur génère un certificat de transaction auquel il associe le montant de transaction, en clair,

- l'utilisateur reçoit, par l'intermédiaire d'un deuxième support de transmission (par exemple téléphone portable ou pageur), ce certificat de transaction et le montant de la transaction en clair,

- il vérifie l'intégrité du montant,

- il tape ces éléments sur le clavier de son terminal, et

- la transaction est ensuite effectuée selon des procédures bancaires connues.

Pour l'information (textes, images, graphiques, sons) et les logiciels fournis à la demande, le réseau utilisé est le réseau mondial connu sous le nom d'"internet". L'objectif de cette application de l'invention est de faire payer à l'acte la

personne qui accède à une ressource à valeur ajoutée et, de lui fournir le service demandé (transmission d'information ou de logiciel) en temps réel.

Dans cette application,

- l'utilisateur se met en relation avec le fournisseur de service,
- il s'identifie en fournissant un identifiant,
- il choisit une information ou un logiciel qui l'intéresse,
- le fournisseur de service indique le prix du service considéré,
- l'utilisateur confirme sa volonté d'achat,
- l'utilisateur reçoit, par l'intermédiaire d'un deuxième support de transmission (par exemple téléphone portable ou pageur), un certificat de transaction assorti du montant de la transaction en clair, et
- il vérifie l'intégrité du paiement,
- il tape le certificat de transaction sur le clavier de son terminal,
- le certificat de transaction est vérifié,
- il reçoit l'information ou le logiciel considéré, et
- il est facturé par relevé mensuel par son opérateur de télécommunication.

Pour l'application à la prise de paris à distance, le réseau utilisé est le réseau mondial connu sous le nom d'"internet". L'objectif de cette application de l'invention est de s'assurer que la personne misant sur un jeu ou prenant un pari à distance est habilitée à le faire et qu'elle a acquitté au préalable les droits nécessaires pour ce jeu.

Dans cette application :

- l'utilisateur ouvre et provisionne son compte chez l'opérateur de service, soit en déposant une somme sur son compte depuis un point de vente quelconque ou par chèque, soit en utilisant la même méthode que dans les applications de l'invention détaillée ci-dessus pour le paiement en ligne,
- puis, lorsque l'utilisateur veut participer à un jeu ou prendre un pari :
- il s'identifie en fournissant un identifiant, et/ou un numéro d'abonné,
- il sélectionne le jeu sur lequel il souhaite miser,

- l'utilisateur reçoit, par l'intermédiaire d'un deuxième support de transmission (par exemple téléphone portable ou pageur), un certificat de transaction assorti de la mise et du pari, en clair, et

- il vérifie la mise et le pari

- il tape le certificat de transaction sur le clavier de son terminal,

- le certificat de transaction est vérifié (mise, pari, chiffres, combinaison).

Pour l'application de l'invention à la fourniture d'offres personnalisées, le réseau utilisé est le réseau mondial connu sous le nom d'"internet". L'objectif de cette application d'identifier les demandes du consommateur en amont de l'acte d'achat et de lui faire des offres personnalisées correspondant à sa demande.

Dans cette application, lors de sa première connexion :

- le consommateur se met en relation avec le service,

- il s'identifie en fournissant un identifiant et/ou un numéro d'abonné,

- il reçoit, par l'intermédiaire d'un deuxième support de transmission (par exemple téléphone portable ou pageur), un mot de passe jetable,

- il tape le mot de passe jetable sur le clavier de son terminal, et

- il remplit un questionnaire marketing permettant de définir les types de propositions commerciales à lui adresser.

Lorsqu'une proposition commerciale correspondant à sa demande lui est adressée, le consommateur reçoit un message "d'alerte", par l'intermédiaire du deuxième support de transmission. Au cours de la deuxième connexion :

- le consommateur se met alors en relation avec le service,

- il s'identifie en fournissant un identifiant et/ou un numéro d'abonné,

- il reçoit, par l'intermédiaire d'un deuxième support de transmission, un certificat de message,

- il tape le certificat de message sur le clavier de son terminal,

- il accède à la boîte aux lettres personnelle et confidentielle qui contient la proposition commerciale,

- il consulte la proposition.

REVENDICATIONS

1. Procédé de transmission d'information sur un premier support de transmission, caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de transmission,

et, durant ladite session :

. une opération de réception d'une information confidentielle sur un terminal à adresse unique sur un deuxième support de transmission, et

. une opération de transmission, sur le premier support de transmission, d'un message confidentiel représentatif de ladite information confidentielle.

2. Procédé de transmission d'information sur un premier support de transmission, caractérisé en ce qu'il comporte :

- une opération d'ouverture, par l'intermédiaire d'un terminal à adresse unique sur ledit premier support de transmission, d'une session de communication avec un moyen de communication situé à distance,

et, durant ladite session :

. une opération de réception d'une information confidentielle sur le premier support de transmission, et

. une opération de transmission, sur un deuxième support de transmission, d'un message confidentiel représentatif de ladite information confidentielle.

3. Procédé de transmission d'information sur un premier support de transmission, caractérisé en ce qu'il comporte :

- une opération d'ouverture, par l'intermédiaire d'un premier terminal, d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de transmission,

- une opération d'ouverture, par l'intermédiaire d'un deuxième terminal, d'une session de communication avec un moyen de communication situé à distance, sur un deuxième support de transmission,

- lorsque les deux sessions sont ouvertes, une opération de réception d'une information confidentielle sur un desdits supports de transmission sur lequel l'un des terminaux a une adresse unique, et

- une opération de transmission, sur l'autre desdits supports de transmission, d'un message confidentiel représentatif de ladite information confidentielle.

4. Procédé de transmission d'information sur un premier support de transmission, caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de transmission,

et, durant ladite session :

. une opération de génération d'une information confidentielle et de transmission de ladite information confidentielle, à un terminal à adresse unique sur un deuxième support,

. une opération de réception, sur le premier support de transmission, d'un message confidentiel susceptible d'être représentatif de ladite information confidentielle, et

. une opération de vérification de correspondance entre ledit message confidentiel et ladite information confidentielle.

5. Procédé de transmission d'information sur un support de transmission dit "deuxième", ledit support de transmission faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un terminal dit "deuxième", d'un premier message représentatif :

. d'un identifiant d'un terminal dit "troisième" possédant une adresse unique sur ledit réseau,

. d'une information confidentielle,

. d'une information représentative d'un montant de transaction,

- une opération de transmission, au troisième terminal, d'un deuxième message représentatif :

. de ladite information confidentielle et

. dudit montant,

- une opération de réception d'un troisième message, de la part dudit deuxième terminal, représentatif d'une validation de transaction, et

- une opération d'incrémentation d'un registre correspondant audit troisième terminal, d'une valeur représentative d'une durée de la première session.

6. Procédé de transmission d'information sur un support de transmission dit "deuxième", ledit support de transmission faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un terminal dit "deuxième", d'un premier message représentatif :

. d'un identifiant d'un terminal dit "troisième" possédant une adresse unique sur ledit réseau,

. d'une information confidentielle,

. d'une information représentative d'un montant de transaction,

- une opération de transmission, au troisième terminal, d'un deuxième message représentatif :

. de ladite information confidentielle et

. dudit montant,

- une opération d'incrémentation d'un registre correspondant audit troisième terminal, d'une valeur prédéterminé.

7. Procédé de transmission d'information sur un support de transmission dit "deuxième", ledit support de transmission faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un terminal dit "deuxième", d'un premier message représentatif :

. d'un identifiant d'un terminal dit "troisième" possédant une adresse unique sur ledit réseau,

. d'une information confidentielle,

. d'une information représentative d'un montant de transaction,

- une opération de transmission, au troisième terminal, d'un deuxième message représentatif :

. de ladite information confidentielle et

. dudit montant,

- une opération de réception d'un troisième message, de la part dudit deuxième terminal, représentatif d'une validation de transaction, et

- une opération d'incrémentation d'un registre correspondant audit troisième terminal, d'une valeur représentative dudit montant de transaction.

8. Procédé de transmission d'information, entre un premier et un deuxième terminal, sur un premier support de transmission appartenant à un réseau de communication, caractérisé en ce qu'il comporte :

- une opération d'ouverture de session de communication, sur le premier support de transmission entre le premier et le deuxième terminal et

- une opération de transmission, de la part du deuxième terminal à un troisième terminal raccordé à un deuxième réseau et possédant une adresse unique sur ledit deuxième réseau, d'un premier message représentatif d'une information confidentielle,

- une opération de transmission, à une adresse sur ledit réseau qui correspond audit troisième terminal d'un deuxième message représentatif de ladite information confidentielle, et

- une opération de transmission, sur le premier support de transmission, en provenance du premier terminal et à destination du deuxième terminal, d'un message représentatif de l'information confidentielle.

9. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 8, caractérisé en ce que l'information confidentielle est représentative d'un montant de transaction.

10. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 9, caractérisé en ce que l'information confidentielle est représentative d'un numéro de session attribué à ladite session.

11. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 10, caractérisé en ce que l'information confidentielle est représentative d'un nombre pseudo-aléatoire.

12. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 10, caractérisé en ce que l'information confidentielle est représentative de l'heure et la date de ladite opération d'ouverture de session.

13. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 10, caractérisé en ce que l'information confidentielle est représentative d'un identifiant de l'utilisateur.

14. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 11, caractérisé en ce que l'information confidentielle est modifiée à chacune des sessions.

15. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 14, caractérisé en ce que l'information confidentielle est représentative d'un ou plusieurs numéros de compte bancaire et/ou de carte de paiement.

16. Serveur informatique, caractérisé en ce qu'il est adapté à mettre en oeuvre le procédé de transmission selon l'une quelconque des revendications 1 à 15.

1/9

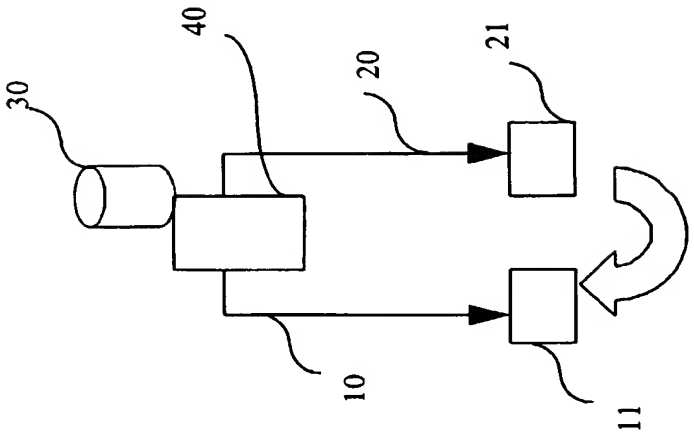


Fig 1

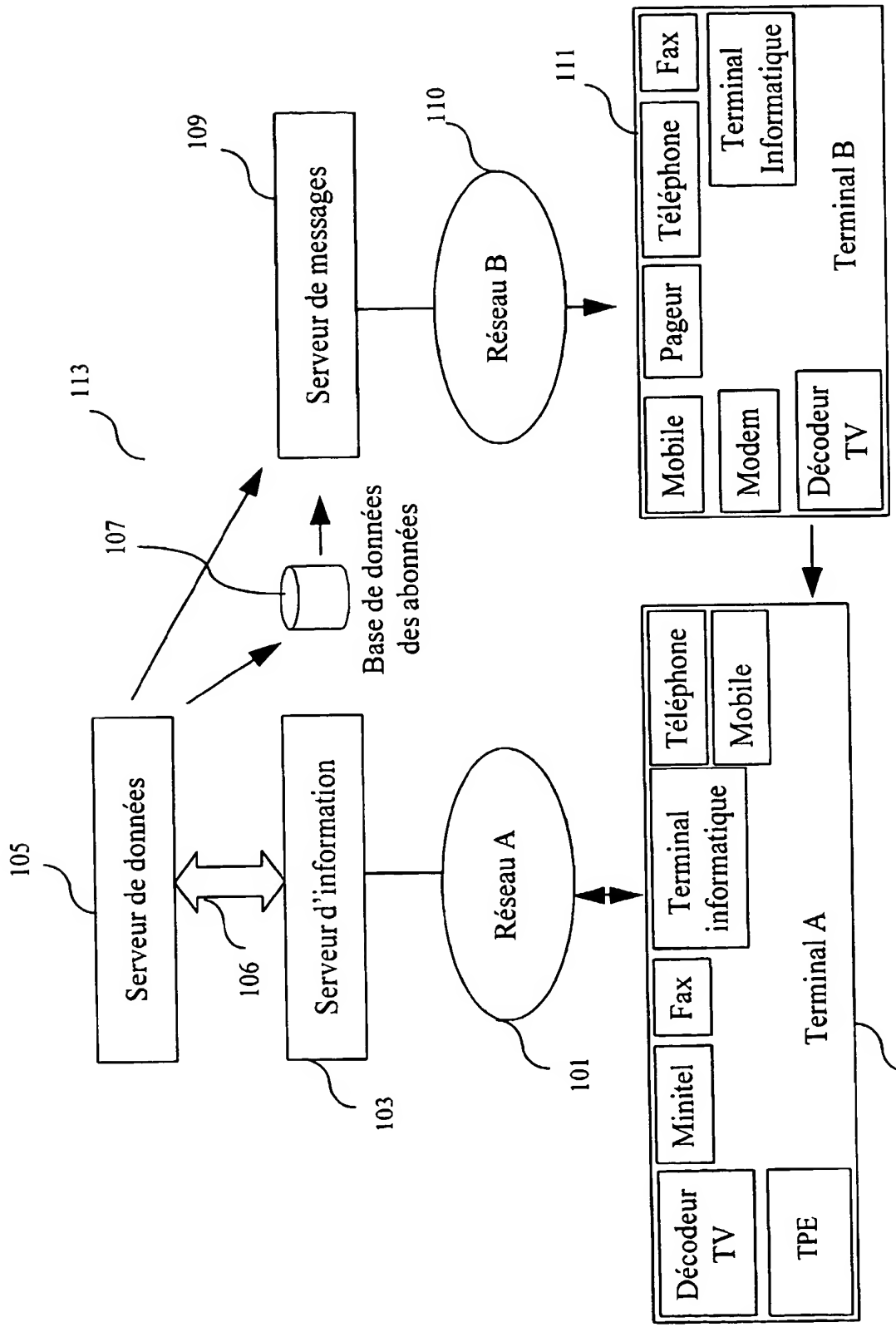


Fig. 2

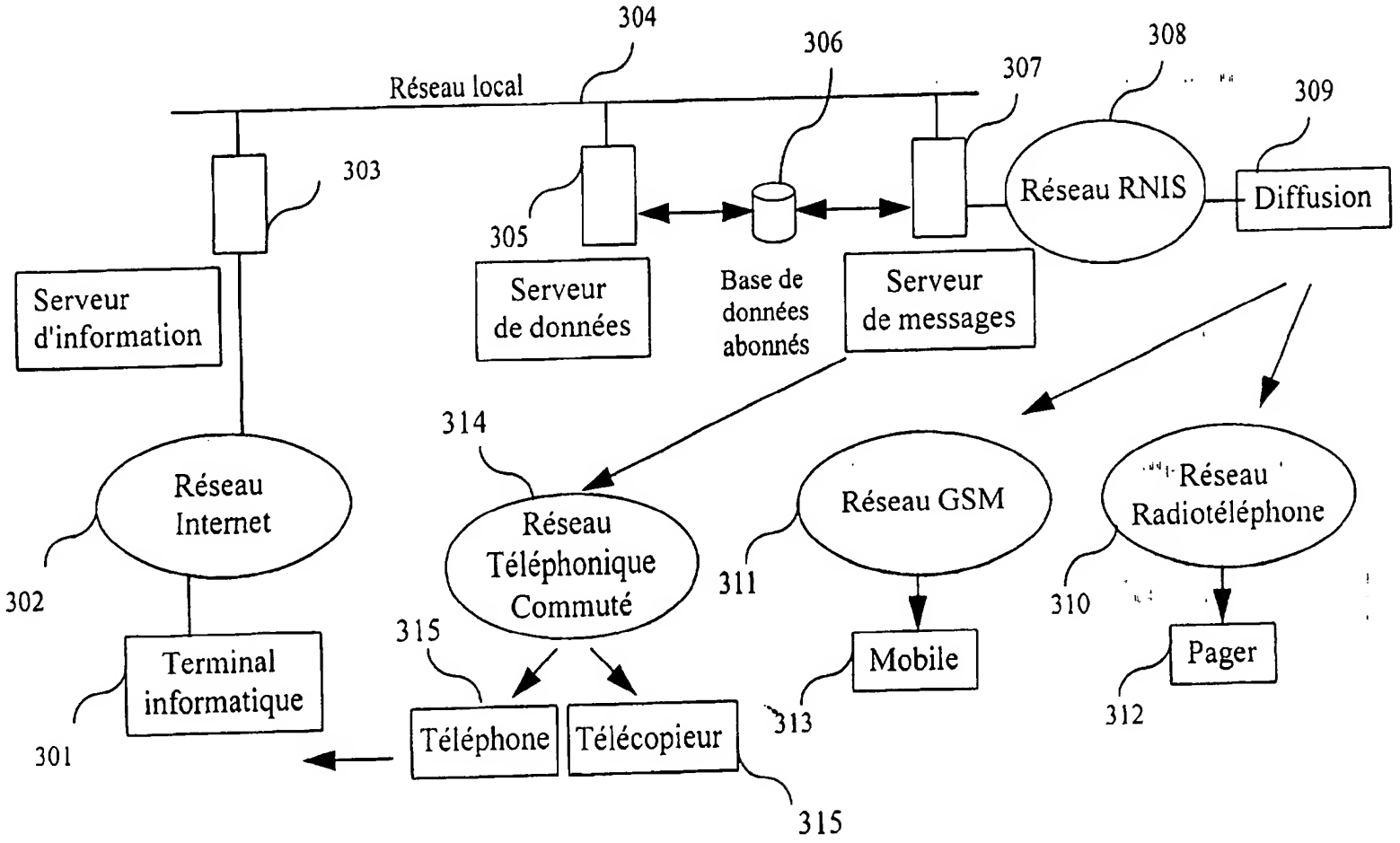


Fig. 3

3/9

2771875

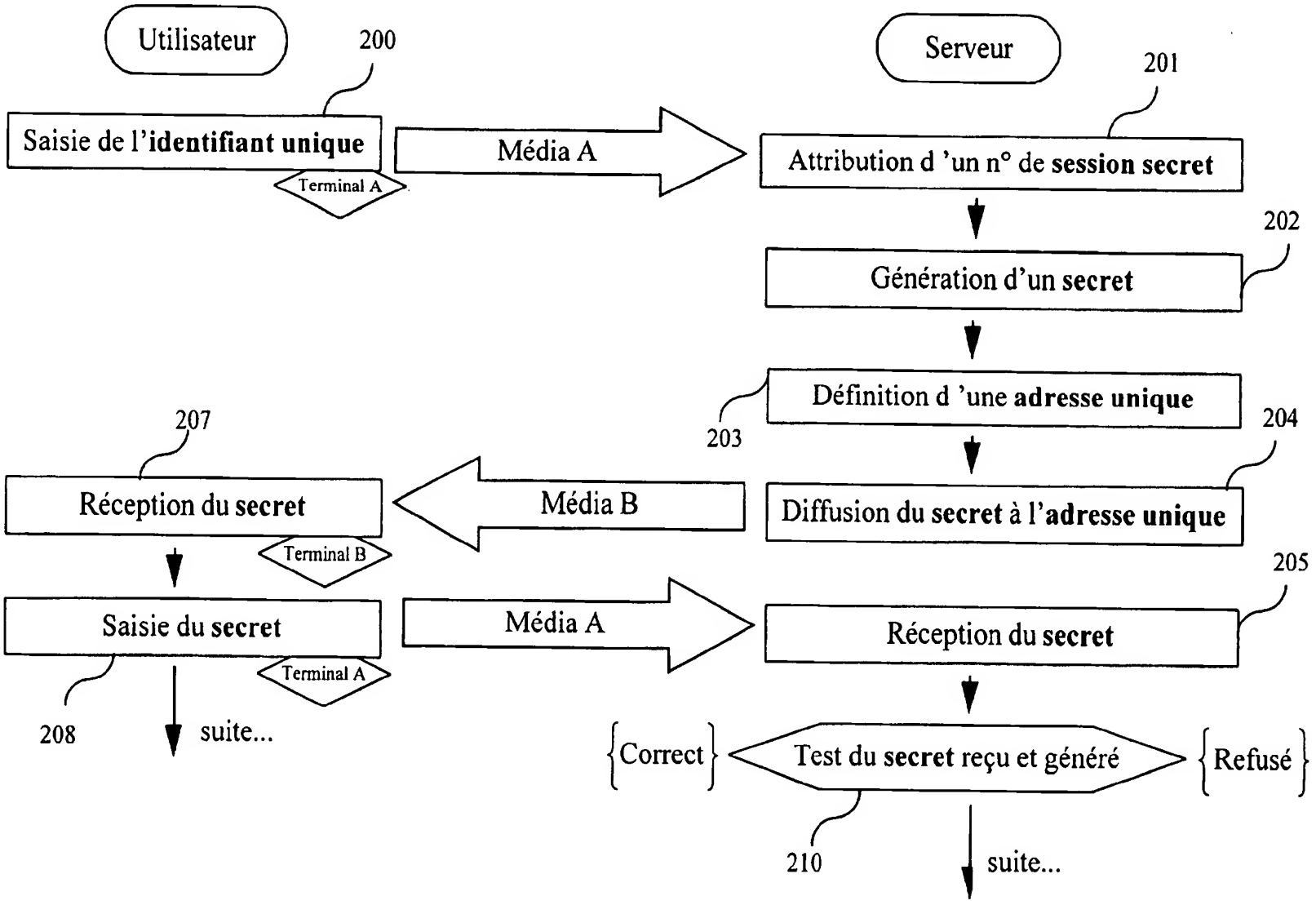


Fig. 4

2771875

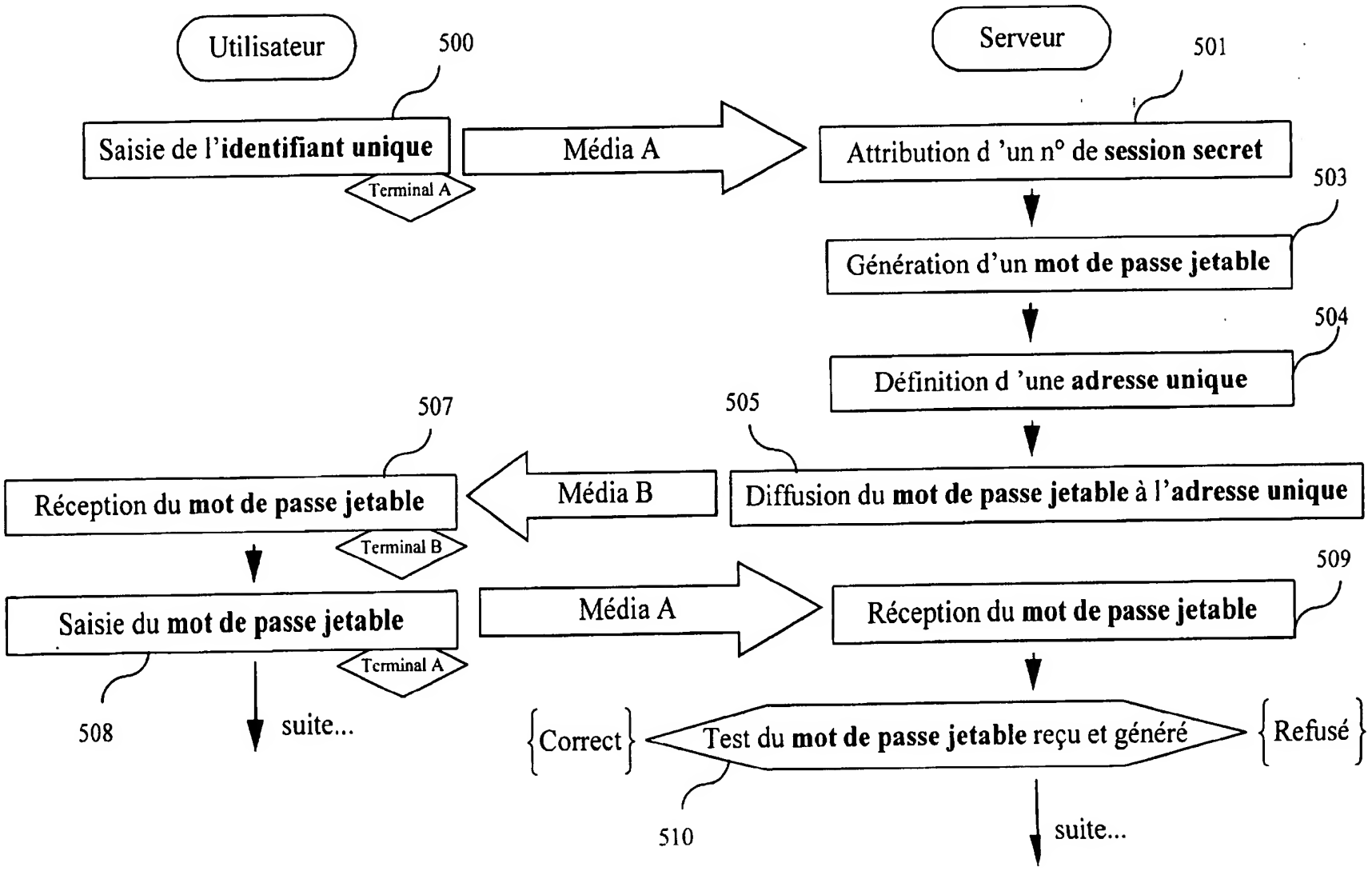


Fig. 5

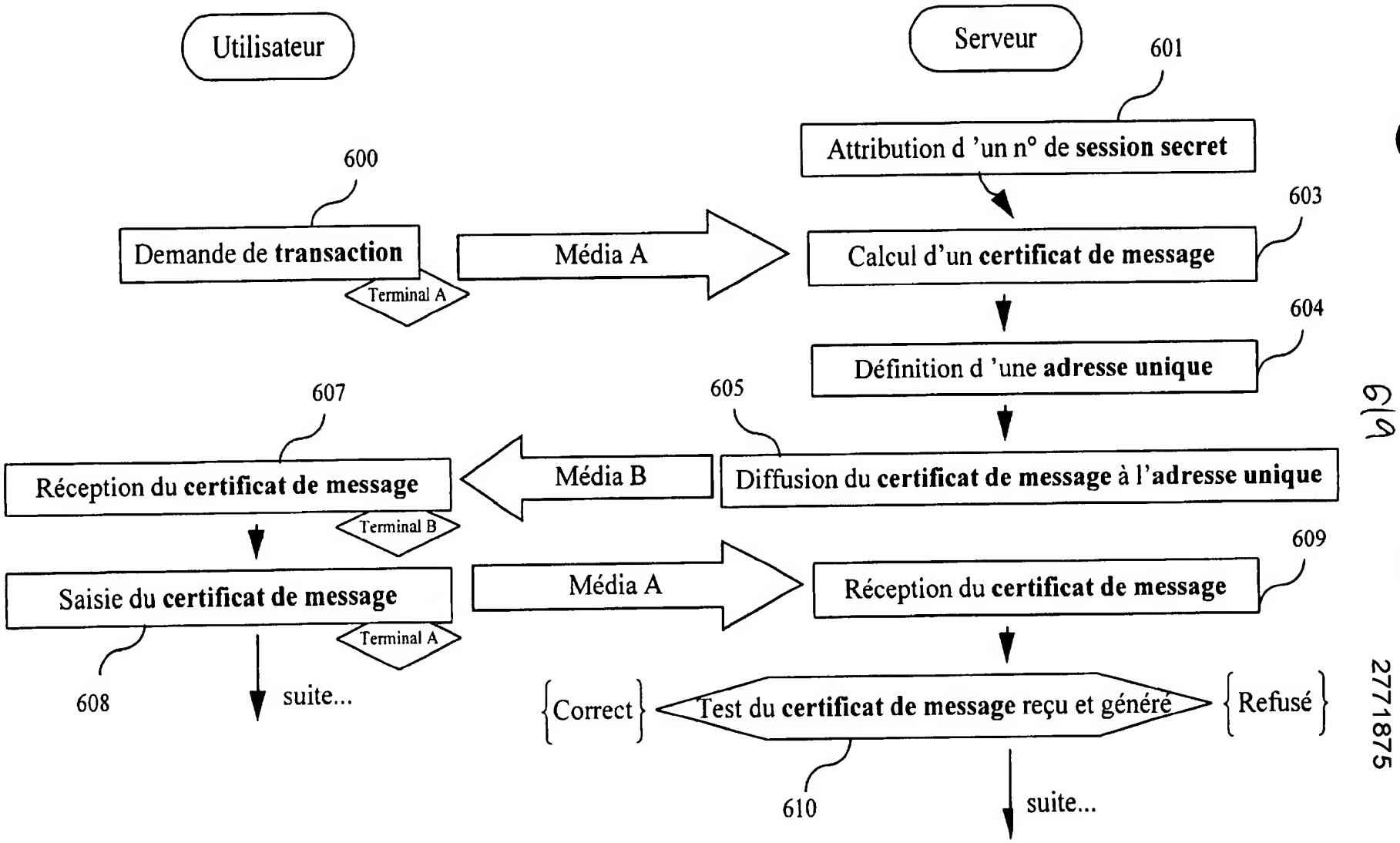


Fig. 6

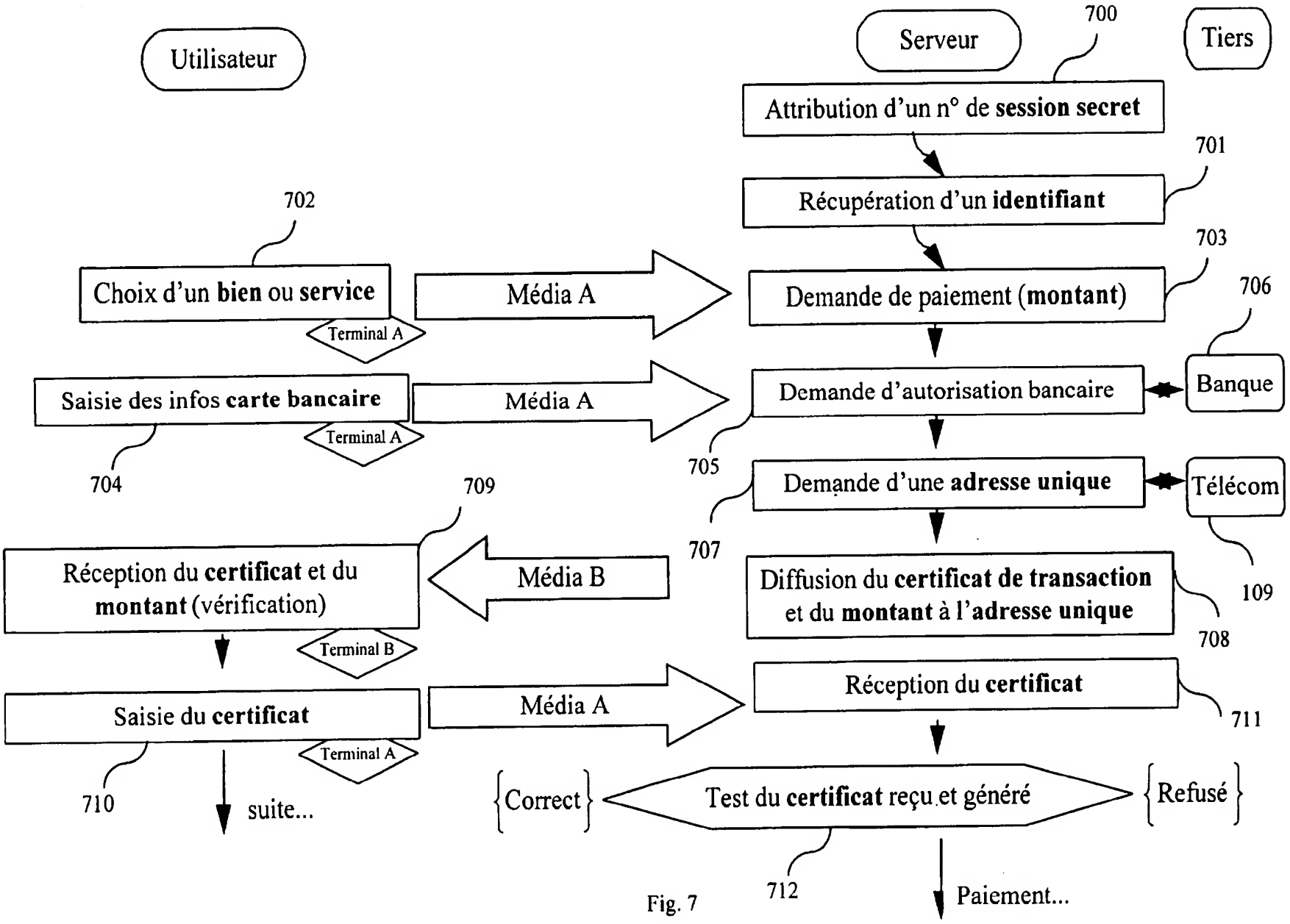

Utilisateur
Serveur
700
Tiers
Attribution d'un n° de session secret
701
Récupération d'un identifiant
702
Choix d'un bien ou service
Terminal A
Média A
703
Demande de paiement (montant)
706
Saisie des infos carte bancaire
Terminal A
Média A
Demande d'autorisation bancaire
Banque
704
705
Demande d'une adresse unique
Télécom
707
709
Réception du certificat et du montant (vérification)
Terminal B
Média B
Diffusion du certificat de transaction et du montant à l'adresse unique
109
708
Saisie du certificat
Terminal A
Média A
Réception du certificat
711
710
suite...
Correct
Test du certificat reçu et généré
Refusé
712
Paiement...

Fig. 7

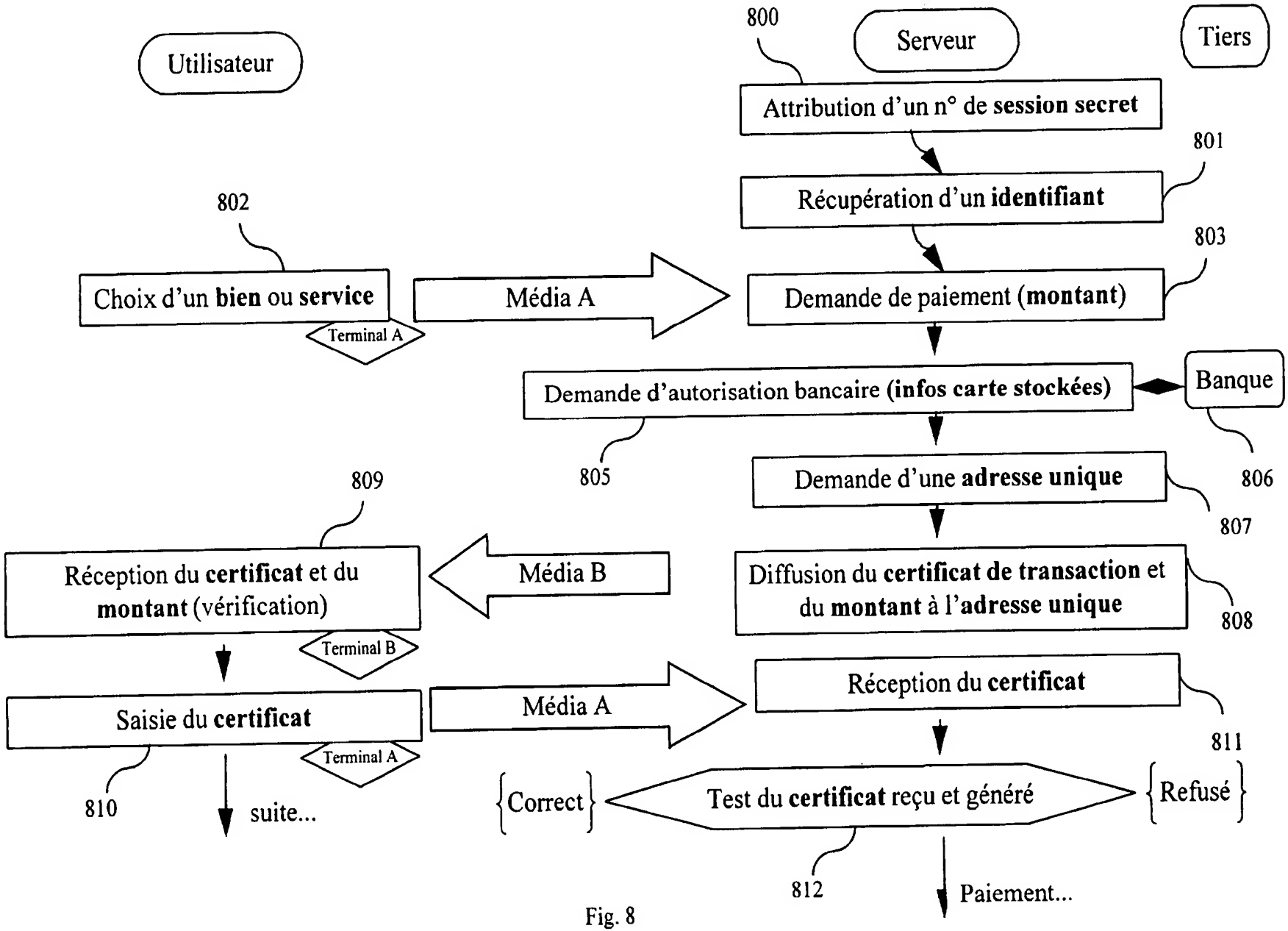


Fig. 8

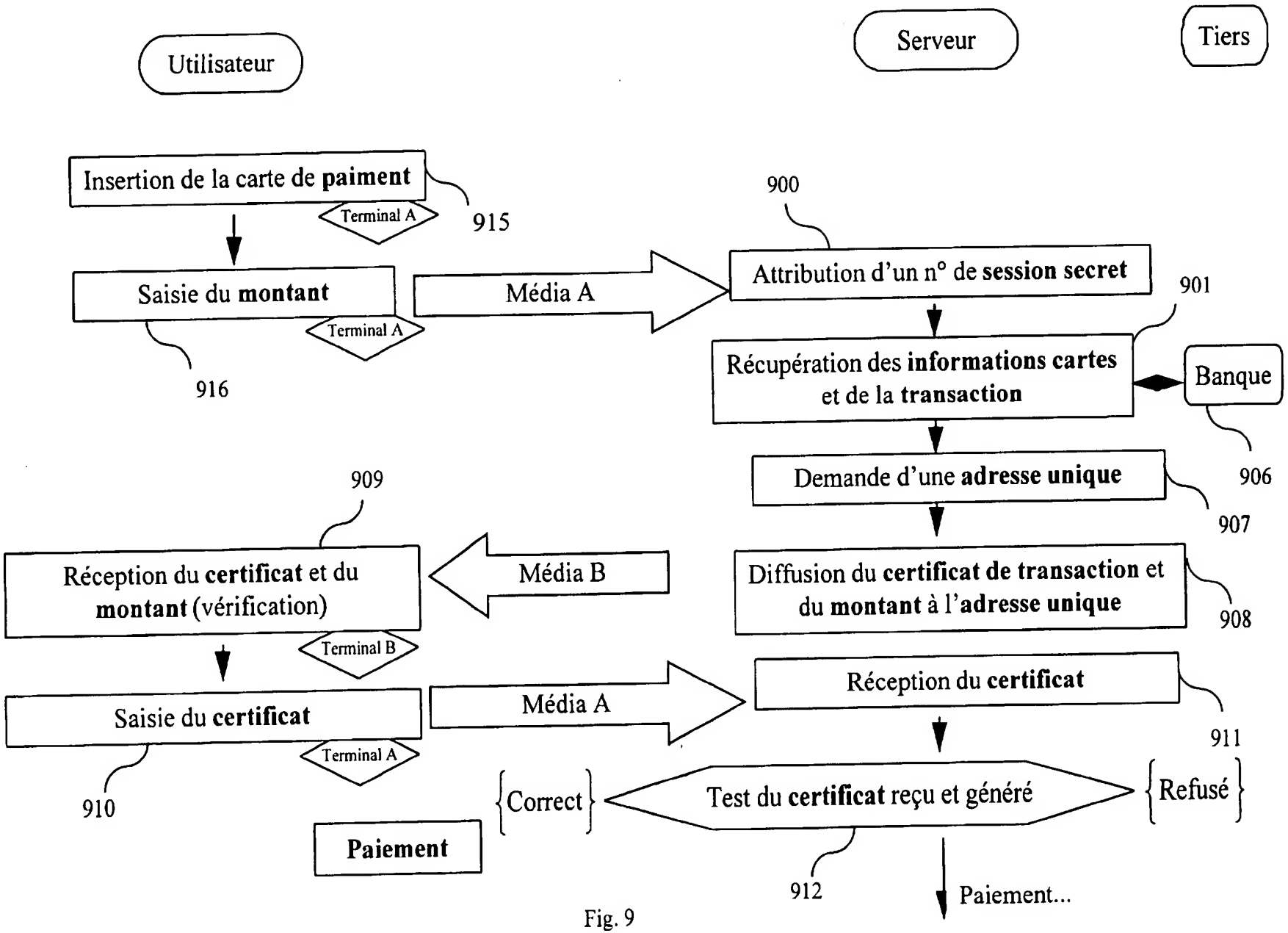


Fig. 9

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2771875

N° d'enregistrement national

FA 549660
FR 9713825

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	EP 0 745 961 A (AT & T CORP) 4 décembre 1996 * colonne 5, ligne 15 - colonne 16, ligne 31; revendications 1-35; figures 1,7-14 * ---	1-8
A	EP 0 416 482 A (HITACHI LTD) 13 mars 1991 * le document en entier * ---	1-10, 13-16
A	WO 96 38962 A (SIEMENS AG ;STEIN KARL ULRICH (DE); HUSSMANN HEINRICH (DE); THEIME) 5 décembre 1996 * abrégé; revendications 1-11; figures 1-6 * ---	1-3
A	US 5 479 510 A (OLSEN KURT B ET AL) 26 décembre 1995 * le document en entier * ---	1-5, 8-10,13, 15,16
A	US 5 371 797 A (BOCINSKY JR RONALD V) 6 décembre 1994 * abrégé; revendications 1-9; figures 1-4 * ---	1-4, 6-13,15, 16
A	EP 0 565 279 A (AMERICAN TELEPHONE & TELEGRAPH) 13 octobre 1993 * abrégé; figures * ---	1
A	WO 95 30975 A (FRANCE TELECOM ;POSTE (FR); COGECOM (FR); PAILLES JEAN CLAUDE (FR)) 16 novembre 1995 * page 6, ligne 11 - page 12, ligne 20 * ---	1
A	US 4 601 011 A (GRYNBERG AVIGDOR) 15 juillet 1986 --- -/--	1

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)
G07F

Date d'achèvement de la recherche	Examinateur
17 juillet 1998	Guivol, O

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2771875

N° d'enregistrement national

FA 549660
FR 9713825

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	WO 94 12954 A (WILSON SHEILA) 9 juin 1994	

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

Date d'achèvement de la recherche	Examinateur
17 juillet 1998	Guivol, O

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

1

EPO FORM 1503 03.82 (P04C13)